General Renuart is the Commander, North American Aerospace Defense Command, and U.S. Northern Command, Peterson Air Force Base, Colorado Springs, Colorado.

Captain Egli is assigned to the Northern Command's Future Operations Division and serves as an operational manager for Maritime Joint Capability Technology Demonstrations.

Naval War College Review, Spring 2008, Vol. 61, No. 2

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Closing the Capability Gap: Developing New Solutions to Counter Maritime Threats	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval War College,686 Cushing Road,Newport,RI,02841-1207**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**11**	

CLOSING THE CAPABILITY GAP

Developing New Solutions to Counter Maritime Threats

General Victor E. Renuart, Jr., USAF, and Captain Dane S. Egli, USCG

> *We face a brutal enemy that has already killed thousands in our midst, and is determined to bring even greater destruction to our shores. . . . Since 9/11, al Qaeda and its allies have succeeded in carrying out horrific attacks across the world; al Qaeda leaders have repeatedly made clear they intend to strike our country again.*
>
> PRESIDENT G. W. BUSH, MAY 2007[1]

America is engaged in a fight against violent extremism, an asymmetric war that differs from any other war our nation has fought. The nature of the enemy has changed dramatically during the past two decades, compelling leaders to reexamine our nation's vulnerabilities in the air, land, and maritime domains. Significant strides have been made nationally to protect the air and land domains against enemy attacks; nonetheless, this article argues, efforts to secure the maritime domain—although improving—are inadequate, and we need to sharpen our focus on maritime threats, domestically and internationally.

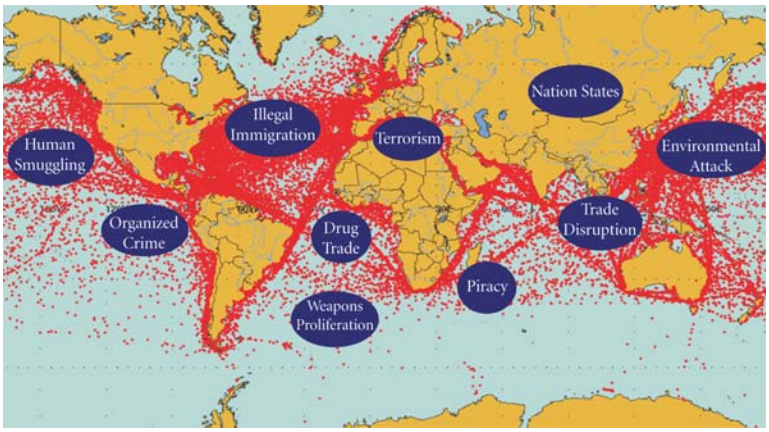
This article draws from the perspective of U.S. Northern Command (USNORTHCOM), whose mission is to anticipate and conduct homeland defense and civil support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests. The article will summarize national-level maritime doctrine, examine the current maritime threat, and introduce new capabilities being developed to counter terrorism on the maritime front—an enduring national security challenge gaining increased attention at all levels.

AMERICA AT RISK

The global security environment is far more uncertain since the end of the Cold War and the emergence of a new, more elusive threat in the form of Islamic extremism, "a transnational movement fueled by a radical ideology of hatred, oppression, and murder," in concert with increased technology and globalization.[2]

This dramatic shift in global security conditions has created vulnerabilities that have been exploited by terrorists in multiple attacks conducted against the United States and its interests.

FIGURE 1
GLOBAL MARITIME CHALLENGES



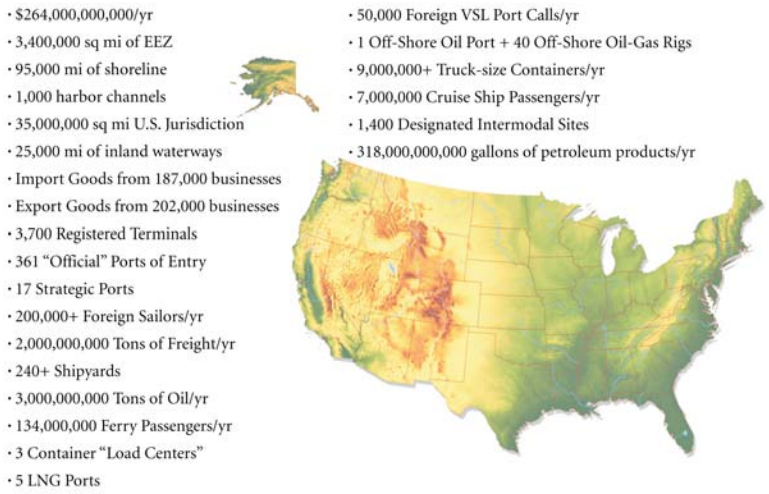
Accordingly, terrorists associated with al Qaeda have exploited national and international vulnerabilities to achieve their goals through acts involving car bombs, commercial airplanes, suicide bombers, and other terrorist methods. Terrorists have demonstrated that they can strike targets of opportunity when and where the nation is least prepared to defend or respond, and, as many counterterrorism experts have asserted, U.S. maritime interests are particularly vulnerable targets. Additionally, an attack on our maritime assets can lead to significant impacts on American and global commerce.

UNIQUE MARITIME VULNERABILITIES

International trade—and especially America's economic vibrancy—depends heavily upon secure and reliable maritime transportation and commerce:[3]

- Globally, maritime trade constitutes over 75 percent of all international trade.
- The United States is a maritime nation, with ninety-five thousand miles of shoreline, 361 commercial ports, and a lucrative economic exclusion zone.
- America conducts 95 percent of its commercial trade (total imports and exports) via maritime conveyances.
- The maritime industry is supported by five hundred container carriers and more than 2,400 container vessels, with approximately 215 million container shipments conducted each year.
- This translates into 11.5 million containers arriving at American ports each year, moving 2.4 billion tons of cargo.
- Over eight thousand foreign vessels conduct over fifty thousand U.S. port visits each year to support this level of trade.
- Some 1,200 to 1,500 commercial vessels call on American ports daily.

FIGURE 2
AN ECONOMY LINKED TO MARITIME COMMERCE...



These statistics highlight the volume of global maritime trade and significance of security challenges in the maritime domain. They point to "soft targets" that terrorists might choose to exploit in attacks against U.S. ports and shipping or by importation of weapons of mass destruction into those ports. The current fragmentation of our capability to monitor commercial vessels, cargo, groups of people, and associated infrastructures further complicates securing maritime systems and the global supply chain.

MARITIME POLICY GUIDANCE

The National Security Strategy clearly states America's strategic imperative to counter terrorism and other threats using all means of national power in response to the terrorist threat and the threat posed by rogue state actors.[4] Since 9/11, and especially since mid-2003, the federal government has been very active in developing maritime policy and assigning organizational responsibilities to provide maritime security. These efforts represent unprecedented steps to achieve greater maritime situational awareness, coordination, intelligence integration, and threat response. They have strengthened our national posture in the maritime domain.

Since mid-2004 there has been a coordinated series of events, starting with the Maritime Domain Awareness Summit, attended by all stakeholders in the federal government, to develop a coherent organizational plan for the defense of national maritime assets. That summit led to the president's release in December 2004 of the Maritime Security Policy, National Security President Directive 41 (NSPD-41), and Homeland Security Directive 13 (HSPD-13), which directed the writing of the *National Strategy for Maritime Security* (NSMS) and its eight supporting plans. The National Security Council, with strong interagency participation, led the effort to develop the NSMS, which addressed the key challenge of achieving a capability to track quickly and accurately commercial vessels, cargo, groups of people, and associated infrastructures. The NSMS, signed by the president in 2005, included both international and interagency aspects and is being

FIGURE 3
NATIONAL STRATEGY FOR MARITIME SECURITY SUPPORTING PLANS

- National plan to achieve Maritime Domain Awareness (MDA)
- Global Maritime Intelligence Integration (GMII)
- Maritime Operational Threat Response (MOTR)
- International Outreach and Coordination Strategy
- Maritime Infrastructure Recovery
- Maritime Transportation System Security
- Maritime Commerce Security
- Domestic Outreach

implemented through the eight supporting plans. The strategy directs the federal government to establish capabilities and mechanisms to achieve heightened maritime security.[5] USNORTHCOM's role included coauthoring a "Concept of Operations" for Maritime Domain Awareness (MDA) with the U.S. Coast Guard.

In combination, these national policies, as instruments of governance, provide the necessary guidance to conduct maritime planning. However, there needs to be a complementary and proactive effort to develop automated systems and rule sets, informed by these policies, representing the information technology and collaborative tools necessary to put MDA into action and produce actionable intelligence. There is clearly a need to implement a comprehensive, fully integrated intelligence/information system that provides greater protection by detecting, analyzing, and reporting global maritime threats.

Two organizations were created specifically to address both the classified and unclassified challenges posed by these tasks. One, directed by the Global Maritime Intelligence Integration Plan, resides in the office of the Director, National Intelligence. The other, created by the National Maritime Domain Awareness Concept of Operations (as part of the National Plan to Achieve Maritime Domain Awareness), with the active concurrence of both the National Security Council and the Homeland Security Council, is the National Office for Global Maritime Situational Awareness. These two organizations are charged with coordinating the national MDA effort, working closely with all the combatant commanders (COCOMs), including USNORTHCOM.

CURRENT STATE: WORKING HARDER TO ACHIEVE MDA

Tracking commercial vessels, cargo, and people, understanding associated infrastructures, and establishing potential relationships among them presents a difficult and time-intensive challenge. Much of today's intelligence concerning maritime data must be manually generated and correlated to determine the threat picture. Analysis of a new "vessel of interest" with current methods is manpower-intensive and can take days. This means a dramatic limitation on the number of ship tracks and volume of related data that can be collected and

analyzed, relative to the tens of thousands of ships that operate daily in the maritime domain.

The lack of standardized data, analytical tools, and data-sharing methodologies (e.g., Service Oriented Architecture) among our maritime partners complicates the correlation process. Most members of the global maritime community of interest independently process various aspects of intelligence data. Other challenges affecting complete visibility of the maritime picture include technical shortfalls of display equipment and policy restrictions on the display of data. For example, the Defense Department possesses baseline Common Operational Picture (COP) tools that facilitate some degree of standardization but were not designed to fuse vessel tracks, cargo, people, and associated infrastructure data. These tools are limited in their ability to exploit new technologies (e.g., incorporation of metadata, use of advanced ship-tracking technologies) and to incorporate information into a comprehensive threat picture. This limitation requires analysts to manually search for and manipulate data, which delays timely information dissemination to combatant commanders and operational decision makers.

Within this context, USNORTHCOM has established linkages with external agencies and intelligence "centers of excellence" to gather maritime threat data. A key partner in this enterprise is the National Maritime Intelligence Center (NMIC), comprising the Office of Naval Intelligence (ONI) and U.S. Coast Guard Intelligence Coordination Center (ICC). NMIC serves as the focal point for USNORTHCOM's maritime threat warning. Further, USNORTHCOM and NMIC rely on a confederated enterprise of maritime intelligence and operations centers for a full threat picture. U.S. Fleet Forces Command, the Joint Force Maritime Component Commander–North, Second Fleet, Third Fleet, and the Coast Guard's Maritime Intelligence Fusion Centers in the Atlantic and Pacific are major partners in this maritime threat analysis and reporting enterprise.

In addition, Canada's partnership in this enterprise is even stronger now that North American Aerospace Defense Command (NORAD) has assumed responsibility for maritime warning for its area of operations. USNORTHCOM, NMIC, and NORAD Headquarters have established avenues for sharing maritime threat information with Canadian organizations, to include Canada Command, Maritime Forces Atlantic, Maritime Forces Pacific, Joint Task Force Atlantic, Joint Force Pacific, and maritime intelligence centers. Collaboration and information sharing are lynchpins of these growing relationships, which further strengthen maritime defense in the hemisphere.

The integration challenges arising from independent databases and inconsistent coordination of maritime information are amplified by the unique jurisdictions, policies, and cultures of each government agency, which further impede

the information sharing and data fusion that could improve MDA capabilities. The United States—specifically, the elements of government associated with maritime services and COCOMs—must address these policy obstacles in order to counter global maritime threats and deter maritime attack.

Within the Defense Department, the USNORTHCOM area of responsibility (AOR) is unique in that it contains the continental United States. Therefore, for missions other than homeland defense, other government agencies (the Homeland Security and Justice departments, etc.) will normally have jurisdiction, with USNORTHCOM operating in a support role for both homeland security and Defense support of civil authorities. Policy hurdles between law enforcement agencies and the Defense Department, as well as the Posse Comitatus Act and intelligence oversight considerations, further limit the department's role in the domestic environment.

Additionally, USNORTHCOM's international partner, NORAD, does not have an area of responsibility. Rather, it has an area of interest that, notably, includes other COCOMs' AORs. Maritime threats to both NORTHCOM's area of responsibility and NORAD's area of interest normally originate overseas, requiring threat analysis to focus initially on other COCOMs' areas of responsibility. Therefore, national intelligence must be fused with interagency and counterintelligence/law enforcement information to fully define the threat. The maritime threat is extraordinarily diverse, ranging from asymmetric sources (international and domestic terrorist groups, rogue states, etc.) to conventional sources (submarine-launched ballistic missiles and conventional naval forces). The question before USNORTHCOM—and the nation—is how to meet emerging operational requirements and resolve policy challenges so as to better counter maritime threats.

FILLING THE GAP

To operate in this unique environment, USNORTHCOM must leverage relationships with critical joint, interagency, and multinational partners. The Office of the Secretary of Defense, USNORTHCOM, U.S. Pacific Command, U.S. European Command, the Naval Research Laboratory, and the Navy's Program Executive Officer for Command, Control, Communications, Computers and Intelligence (PEO C4I) are collectively leading an effort to develop an MDA technical capability to share maritime databases in a manner that delivers automated ship-tracking tools and fused metadata in a User-Defined Operational Picture (UDOP). This new technology will provide Web-based dissemination and collaboration capability across multiple security levels to ensure that mission partners worldwide have access to global maritime intelligence and information.

This capability, known as Comprehensive Maritime Awareness (CMA) and Maritime Automatic Super Track Enhanced Reporting (MASTER), is being spirally developed through two Joint Capability Technology Demonstrations (JCTDs) sponsored by the Office of the Secretary of Defense and supported by the Joint Requirements Oversight Council and Congress. The CMA initiative will reinforce MDA prototype development across the interagency community and within the U.S. Navy, by providing security analysts with shared information about a broad range of subjects that include vessels, cargo, people, ports, waterways, critical infrastructure, friendly forces, and financial transactions.

The goal of these demonstrations is to automate all-source fusion in order to help maritime intelligence analysts better support the warfighter and respective interagency partners in the field. CMA will be able to fuse multiple sources of data, including the International Maritime Organization–mandated Automated Identification System (AIS), Defense Department and Homeland Security Department systems, and many other national and open sources; the current design includes over three hundred inputs from both U.S. government and public domains. CMA and MASTER will also support maritime anomaly detection, allowing identification of potential threats that currently go undetected and are therefore missing from the "vessel of interest" list. MASTER's capabilities differ from those of CMA in that it will fuse information sources at the highest security levels, using the most sensitive sources of intelligence information.

As mandated by the *National Strategy for Maritime Security*, we must not only leverage interagency capabilities but also build cooperation with international partners in order to identify threats as far from our shores as possible. To that end, the maritime JCTDs are making clear the value of collaboration with allies in parts of the world where maritime traffic and shipping commerce are heavy.

CMA and MASTER will support the transformation of national MDA capabilities by moving maritime information systems

. . . from:

- Manual processes for data acquisition, data validation, correlation, and track generation
- High analytical latency (that is, a need for considerable time to collect data and determine if there is a potential threat)
- Nonstandardized data collection and information-processing protocols, and
- Monitoring of hundreds of named vessels of interest at any given time via a Common Operating Picture

. . . to:

- Automated processes (automatic acquisition, validation, correlation, tracking with identification)
- Reduced latency, improving analytical efficiency by orders of magnitude
- Standardized reporting protocols that support a net-centric Service Oriented Architecture, and
- A focus on threat identification, based on monitoring thousands of vessels at any given time, via a UDOP.[6]

As a result, maritime analysts will spend more of their time analyzing cues, which will be *automatically* generated, rather than *manually* searching intelligence reports and databases to establish suspicious associations among vessels, cargo, infrastructure, and people. Ultimately, analysts and decision makers will be able to devote more attention to the most likely threats, many of which today would likely not be listed as vessels of interest.

FUTURE STATE: WORKING SMARTER TO ACHIEVE MDA

Given the anticipated technological advances described above, especially CMA and MASTER, the time needed to generate maritime threat intelligence will significantly decrease. Gathering, correlating, and fusing critical maritime information will take hours rather than days, as it can today. Maritime situational awareness will be greatly enhanced as a result. The Service Oriented Architecture requirement will lay out a path to data interoperability and data sharing, ensuring that participating analysts in the global maritime community of interest can assimilate data from participating joint, interagency, and industry providers.

These tools, coupled with emerging organizational constructs—for instance, the Navy's Maritime Headquarters with Maritime Operations Center (MHQ-MOC) and databases such as the U.S. Coast Guard's Maritime Awareness Global Network (MAGNET)—will streamline command and control capabilities, facilitating more rapid MDA for senior decision makers and improved operational response in support of the *National Strategy for Maritime Security*.[7]

In very positive moves forward, the U.S. Navy, the Defense Department's executive agent for Maritime Domain Awareness, is making an effort to accelerate development of MDA prototype capabilities (selecting CMA as a core technology) and is moving toward a specific Program of Record for MDA-related fusion tools.[8] Additionally, the CMA Transition Manager—the Navy's PEO C4I—is working to create a single acquisition program for all battlespace awareness and information operations systems and services. This change will further strengthen

the objectives of delivering integrated C4I capabilities to fleet commanders and of bringing out new innovations to counter global maritime threats.

If we are to exploit fully the maritime joint capability technology demonstrations and advance MDA systems nationally, there remain fundamental challenges concerning how the United States and its allies will develop MDA systems globally. These include:

- How will we expand interagency cooperation within the U.S. government to support integration of MDA-related systems?
- How must the Defense Department interact with interagency partners, as well as state, regional, local, and federal law enforcement authorities?
- How are we to integrate collaborative tools to support the next generation of MDA?
- How are we to integrate the efforts of, and provide access to, international maritime partners, specifically addressing foreign disclosure issues?
- How are we to resolve cross-domain policy issues (security, commercial industry, law enforcement versus the Defense Department versus the intelligence community)?
- How are we to implement and enforce a Service Oriented Architecture and ensure that it supports MDA objectives?
- How are we to address inbound small vessels (under 300 registered gross tons) that are not subject to current reporting requirements, as well as other potentially suspect traffic using inland waterways?

As the regional military leaders, the geographic combatant commanders support national efforts to implement the *National Strategy for Maritime Security* and garner interagency support to establish an MDA Program of Record. Through an expanded and funded MDA program, new technologies can be fielded that support maritime information-sharing systems and the Navy's Maritime Headquarters with Maritime Operations Centers. Multiple MDA initiatives will provide initial technology solutions, but renewed efforts are needed to ensure that cross-domain data sharing and fusion grow into a core capability of national MDA systems in the global maritime community of interest.

CMA and MASTER are two leading maritime initiatives designed to accelerate the development and fielding of follow-on MDA systems. Their residual capabilities will support the emerging MDA architecture needed for data interoperability within the global community—representing a transformational approach to fusing and sharing maritime information.

The sense of urgency in fielding new MDA capabilities is based on the nature of the threat to the nation and its allies, the criticality of protecting the national economy, and a need to assure the public of national security. Only by providing our maritime analysts with automated, more detailed, and comprehensive information can we hope to close the capability gap in global maritime security. These new capabilities will enable detection of maritime threats farther from our shorelines, allow more timely operational decisions, and ultimately prevent in the maritime domain an attack of the magnitude experienced on September 11, 2001. Our *National Security Strategy* states, "We must build and maintain our defenses beyond challenge." It is our nation's strategic imperative to improve situational awareness and secure the maritime domain—before the enemy chooses to challenge us in our harbors, ports, or waterways.

NOTES

1. Speaking at graduation ceremonies at the U.S. Coast Guard Academy, New London, Connecticut, in May 2007.
2. *National Strategy for Combating Terrorism* (Washington, D.C.: White House, National Security Council, September 2006), p. 1.
3. U.S. Navy Dept., *The Cargo Tracking Handbook* (Washington, D.C.: Office of Naval Intelligence, February 2007), pp. 1–7; U.S. Transportation Dept., *Pocket Guide to Transportation* (Washington, D.C.: Bureau of Transportation Statistics, January 2006), pp. 36–37.
4. *The National Security Strategy* (Washington, D.C.: White House, National Security Council, March 2006), pp. 3–7.
5. National Security Presidential Directive 41 (NSPD-41)/Homeland Security Presidential Directive 13 (HSPD-13), 21 December 2004.
6. The technology to build a UDOP is in place. The hard task is to gain the policy accesses and permissions necessary to build it. CMA and related programs are working, with USNORTHCOM's support, to accomplish these goals.
7. MHQ-MOC is a network of U.S. Navy regional MDA nodes designed to execute joint maritime operations and provide connectivity for theater-level maritime requirements. MAGNET is a U.S. Coast Guard maritime database that provides integrated afloat, ashore, and airborne C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) support for vessel tracking and port information.
8. Secretary of the Navy memo, "Maritime Domain Awareness (MDA) Capability," 17 May 2007.